IP-KONFIGURATION UND TROUBLESHOOTING

Inhalt

1. MINDEST-KONFIGURATION EINES IP-KNOTENS 2

2. IP (LAYER 3)-FEHLERARTEN UND FEHLERBILDER 2

3. NÜTZLICHE TOOLS FÜR DIE IP-FEHLERSUCHE 4

3.1. Auffinden von MAC-, IP-Adressen und Host-ID 4

3.2. Netstat 6

3.3. ping - Erreichbarkeitskontrolle für IP-Knoten 7

3.4. route 9

3.5. tracert 10

3.6. Der Befehl pathping 12

3.7. nslookup - Überprüfung der Namensauflösung 12

3.8. nbtstat - NetBIOS Namentests 15

4. NETZWERK-FEHLERSZENARIEN 16

4.1. Fehlerbild: Unerreichbarkeit von IP-Stationen 16

4.2. Fehlerbild: Unerreichbarkeit von IP-Stationen 17

5. ZUSAMMENFASSUNG 19

5.1. Häufige Fehlerursachen bei Koaxialverkabelung (Layer 1): 19

5.2. Häufige Fehlerursachen bei Ethernet (Layer 2): 20

5.3. Häufige Fehlerursachen bei IP (Layer 3): 20

1. MINDEST-KONFIGURATION EINES IP-KNOTENS

Folgende Punkte müssen für einen IP-Netzknoten mindestens konfiguriert werden.

- Physikalischer Anschluß an das Netzwerk: normierte Schnittstelle (physical layer)
- Netzwerk-Adapter mit Aktivierung der Schnittstelle für gewähltes Zugriffsverfahren (MAC-Layer); Identifikation des Adapters über MAC-Adresse
- Vergabe einer eindeutigen IP-Adresse für jeden Netzwerkzugang
- Konfiguration der Subnetzmaske
- Angabe des default-Routers (default-Gateway)

2. IP (LAYER 3)-FEHLERARTEN UND FEHLERBILDER

Das IP als Layer-3-Protokoll hat sich sowohl im Internet als auch bei den meisten Firmen durchgesetzt, deswegen ist es bedeutsam, Layer 3 bzw. IP-Fehlern zu erkennen und detektieren zu können.

Folgende Fehlerursachen treten bei IP häufig auf:

- Doppelte MAC-Adressen (Datenfehler auf dem Netzwerk)
- Doppelte IP-Adressen (IP-Stack bricht zusammen, ping 127.0.0.1 bleibt erfolglos)
- Fehlende oder falsche Angabe des default-Routers (Default-Gateway); Kommunikation aus dem Subnetz heraus ist nicht möglich
- Falsche Konfiguration der Subnetzmaske (Rechner sehen sich nicht)
- TCP/IP nicht korrekt installiert
- falsche IP-Adresse
- Router-Port nicht aktiv
- fehlerhafte Accessliste/Filter auf Router
- unbekanntes Zielnetz
- Netzüberlastung
- Überlastung von Routern (siehe discard ip packets)
- Routerprozess nicht aktiv
- unterschiedliche Timer-Werte für Routingprotokolle bei Routern

Arbeitet man bei einem Problem die Tabelle von oben nach unten ab, können die Ursachen nach und nach ausgeschlossen werden. Mögliche Ursachen von Layer 3 Fehlern sind:

Symptome	Mögliche Ursachen

Ping der Problemstation auf die Loopbackadresse 127.0.0.1 ist	TCP/IP nicht korrekt installiert
Ping der Problemstation auf die eigene IP-Adresse ist erfolglos	TCP/IP nicht korrekt installiert
	Netzwerkkarte defekt
Ping von einem Endgerät im gleichen Subnetz auf die Problemstation ist erfolglos	Problemstation hat falsche IP-Adresse
	Problemstation hat falsche Subnetzmaske
	Problemstation ist nicht am Netz angeschlossen
Ping von der Problemstation auf ein Endgerät im gleichen Subnetz ist erfolglos	Angepingte Station nicht am Netz
	Falsche IP-Adresse beim Ping
	Problemstation ist nicht am Netz angeschlossen
Ping von der Problemstation zum Default-Gateway ist erfolglos	Problemstation ist nicht am Netz angeschlossen
	Problemstation hat eine falsche IP-Adresse
	Problemstation hat eine falsche Subnetzmaske
	IP-Adresse des Default-Gateways ist falsch
	Port am Router ist nicht aktiv
	Default-Router ist nicht am Netz
Ping von der Problemstation zu einem Endgerät in einem anderen Subnetz	Problemstation ist nicht am Netz angeschlossen
	Problemstation hat eine falsche IP-Adresse
	Problemstation hat eine falsche Subnetzmaske
	IP-Adresse des Default-Gateways ist falsch
	Port am Router ist nicht aktiv
	Default-Router ist nicht am Netz
	Accessliste/Filter auf Router erlaubt den Zugriff nicht
	Zielnetz ist am Default-Router unbekannt
	Zielstation ist nicht am Netz angeschlossen
Ping auf eine IP-Adresse funktioniert, Ping auf den Namen	Problem mit der Namensauflösung. Falsche Zuordnung von Name zu IP. DNS-Server unbekannt oder
Verbindung auf IP-Ebene funktioniert, eine Anwendung kann	Accessliste auf Router erlaubt für bestimmte TCP/UDP-Ports den Zugriff nicht.
Zeitweise Verbindungsabbrüche	Doppelte IP-Adresse im Netz
	Überlastung des Netzwerks
	Überlastung von Netzwerkkomponenten
Routing-Problem bei OSPF	OSPF nicht aktiv
	Timer (Hello, Dead) nicht aufeinander abgestimmt
	Router-Port nicht aktiv

Bild: Layer 3 Symptome und mögliche Ursachen

Die Fehlersuche in Netzwerken ist natürlich nicht mit den obigen Tabellen erledigt. Sie können nur als Hilfsmittel zur Vorgehensweise dienen. Bei vielen Problemen ist es nur möglich, über das Ausschlussverfahren zu arbeiten. In der Praxis kann dies dazu führen, dass Teile des Netzwerkes vom restlichen Netz getrennt werden müssen, um den Fehler eingrenzen zu können.

3. NÜTZLICHE TOOLS FÜR DIE IP-FEHLERSUCHE

3.1. Auffinden von MAC-, IP-Adressen und Host-ID

Mit folgenden Kommandozeilenbefehle lässt sich die MAC-Adresse, IP-Adresse und Host-ID ermitteln:

SunOS/Solaris	type the command:	hostid
HPUX	type the command:	uname -i
AIX	type the command:	uname -m
SGI	type the command:	sysinfo -s
Win 95/98	type the command:	winipcfg /all
Win NT/Win2K	type the command:	ipconfig /all
Linux	type the command:	/sbin/ipconfig eth0

Der Befehl arp

Um Fehler bei der Namensauflösung zwischen MAC- und IP-Adressen aufzuspüren, ist der Befehl *arp* hilfreich. Er zeigt die Einträge des arp-Cache an und ermöglicht es, diese anzupassen. Mit *arp -a* erhält man die MAC-Adressen der zuletzt angesprochen IP-Adressen.

Die MAC-Adresse des eigenen Rechners lässt sich durch Eingabe von *ipconfig /all* feststellen.

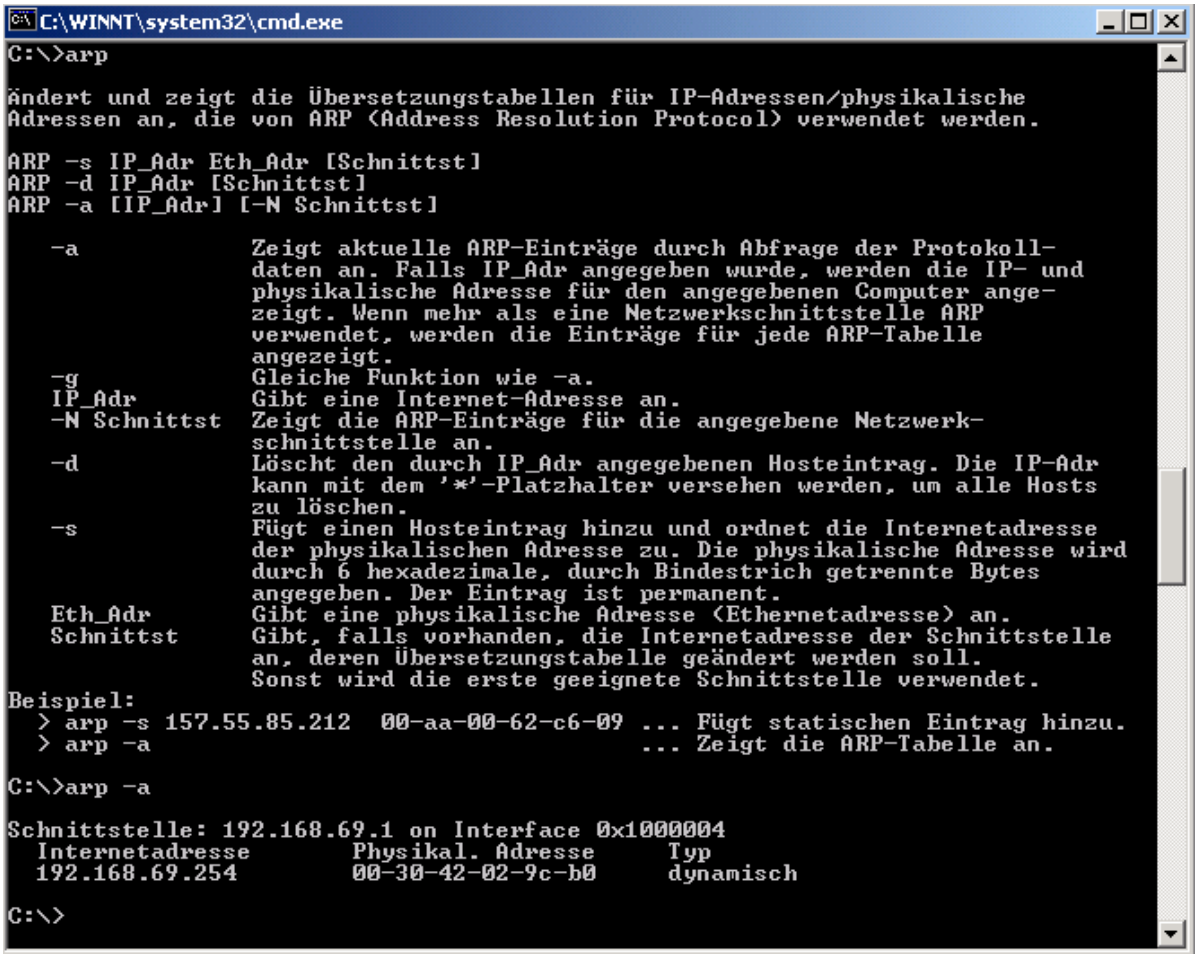

C:\WINNT\system32\cmd.exe
C:\>arp
Ändert und zeigt die Übersetzungstabellen für IP-Adressen/physikalische
Adressen an, die von ARP (Address Resolution Protocol) verwendet werden.
ARP -s IP_Adr Eth_Adr [Schnittst]
ARP -d IP_Adr [Schnittst]
ARP -a [IP_Adr] [-N Schnittst]
-a Zeigt aktuelle ARP-Einträge durch Abfrage der Protokoll-
daten an. Falls IP_Adr angegeben wurde, werden die IP- und
physikalische Adresse für den angegebenen Computer ange-
zeigt. Wenn mehr als eine Netzwerkschnittstelle ARP
verwendet, werden die Einträge für jede ARP-Tabelle
angezeigt.
-g Gleiche Funktion wie -a.
IP_Adr Gibt eine Internet-Adresse an.
-N Schnittst Zeigt die ARP-Einträge für die angegebene Netzwerk-
schnittstelle an.
-d Löscht den durch IP_Adr angegebenen Hosteintrag. Die IP-Adr
kann mit dem '*'-Platzhalter versehen werden, um alle Hosts
zu löschen.
-s Fügt einen Hosteintrag hinzu und ordnet die Internetadresse
der physikalischen Adresse zu. Die physikalische Adresse wird
durch 6 hexadezimale, durch Bindestrich getrennte Bytes
angegeben. Der Eintrag ist permanent.
Eth_Adr Gibt eine physikalische Adresse (Ethernetadresse) an.
Schnittst Gibt, falls vorhanden, die Internetadresse der Schnittstelle
an, deren Übersetzungstabelle geändert werden soll.
Sonst wird die erste geeignete Schnittstelle verwendet.
Beispiel:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 ... Fügt statischen Eintrag hinzu.
> arp -a ... Zeigt die ARP-Tabelle an.
C:\>arp -a
Schnittstelle: 192.168.69.1 on Interface 0x1000004
Internetadresse Physikal. Adresse Typ
192.168.69.254 00-30-42-02-9c-b0 dynamisch
C:\>

Bild: Der Befehl arp

Der Befehl ipconfig

Das Tool *ipconfig* bietet neben der Ausgabe der Netzwerkkonfigurations-Parameter einige weitere nützliche Optionen, um Netzprobleme zu beseitigen.

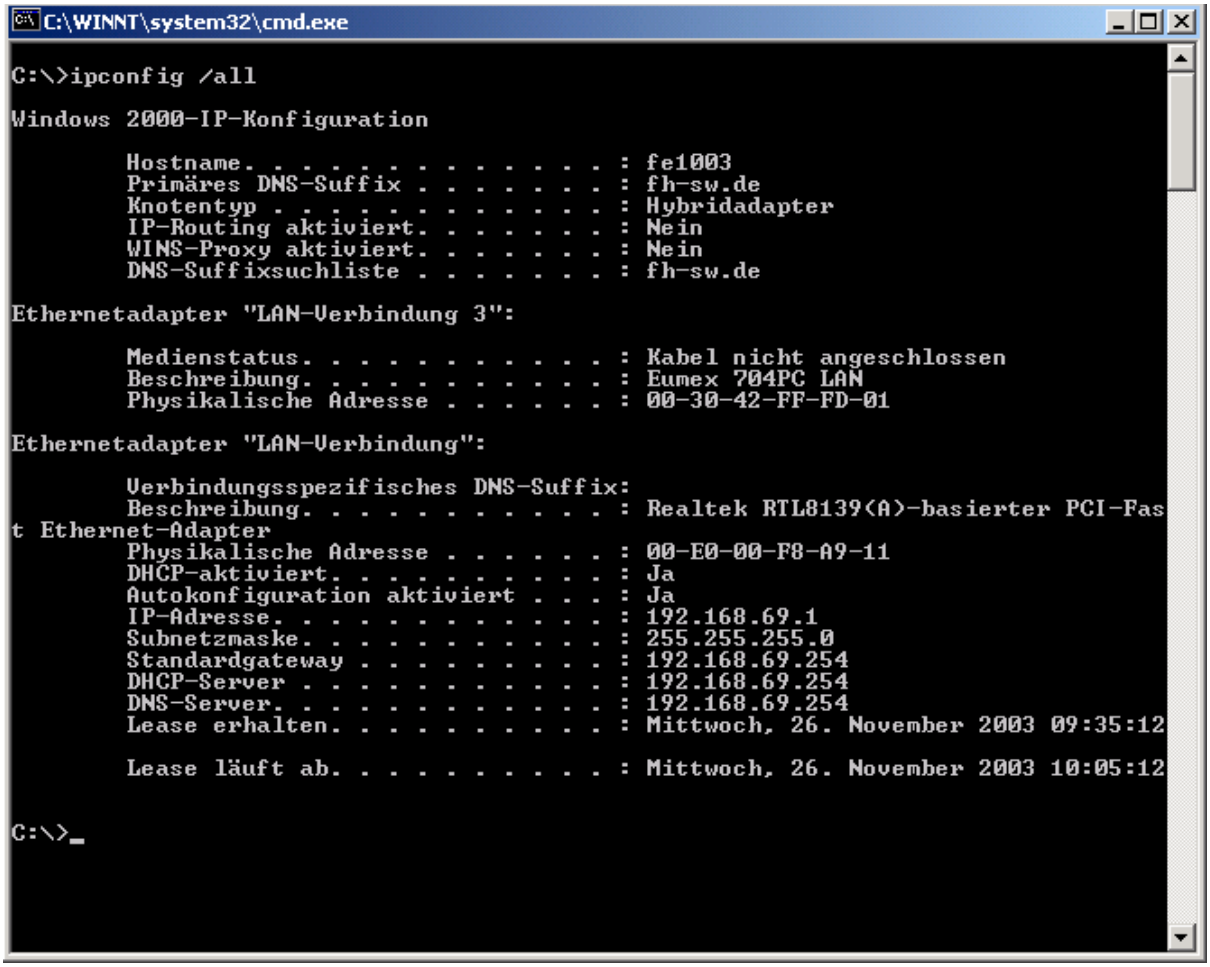

C:\WINNT\system32\cmd.exe
C:\>ipconfig /all
Windows 2000-IP-Konfiguration
Hostname. . . . . : fe1003
Primäres DNS-Suffix . . . . . : fh-sw.de
Knotentyp . . . . . : Hybridadapter
IP-Routing aktiviert. . . . . : Nein
WINS-Proxy aktiviert. . . . . : Nein
DNS-Suffixsuchliste . . . . . : fh-sw.de
Ethernetadapter "LAN-Verbindung 3":
Medienstatus. . . . . : Kabel nicht angeschlossen
Beschreibung. . . . . : Eumex 704PC LAN
Physikalische Adresse . . . . . : 00-30-42-FF-FD-01
Ethernetadapter "LAN-Verbindung":
Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . : Realtek RTL8139(A)-basierter PCI-Fas
t Ethernet-Adapter
Physikalische Adresse . . . . . : 00-E0-00-F8-A9-11
DHCP-aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
IP-Adresse. . . . . : 192.168.69.1
Subnetzmaske. . . . . : 255.255.255.0
Standardgateway . . . . . : 192.168.69.254
DHCP-Server . . . . . : 192.168.69.254
DNS-Server. . . . . : 192.168.69.254
Lease erhalten. . . . . : Mittwoch, 26. November 2003 09:35:12
Lease läuft ab. . . . . : Mittwoch, 26. November 2003 10:05:12
C:\>

Bild: Der Befehl ipconfig /all

Ipconfig /flushdns löscht den DNS-Namens-Cache,

Ipconfig /registerdns erneuert alle DHCP-Leases und registriert die DNS-Namen neu,

Ipconfig /displaydns zeigt alle Einträge an, die im DNS-Resolver-Cache vorhanden sind.

C:\WINNT\system32\cmd.exe
C:\>ping www.arcor.de
Ping www.arcor-online.net [151.189.21.100] mit 32 Bytes Daten:
Antwort von 151.189.21.100: Bytes=32 Zeit=60ms TTL=247
Antwort von 151.189.21.100: Bytes=32 Zeit=60ms TTL=247
Antwort von 151.189.21.100: Bytes=32 Zeit=60ms TTL=247
Antwort von 151.189.21.100: Bytes=32 Zeit=50ms TTL=247
Ping-Statistik für 151.189.21.100:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 50ms, Maximum = 60ms, Mittelwert = 57ms
C:\>ipconfig /displaydns
Windows 2000-IP-Konfiguration
localhost.
Eintragsname. . . . . : localhost
Eintragstyp . . . . . : 1
Gültigkeitsdauer. . . : 31532112
Datenlänge. . . . . : 4
Abschnitt . . . . . : Answer
(Host-) Eintrag . . . :
127.0.0.1
www.arcor-online.net.
Eintragsname. . . . . : www.arcor-online.net
Eintragstyp . . . . . : 1
Gültigkeitsdauer. . . : 601
Datenlänge. . . . . : 4
Abschnitt . . . . . : Answer
(Host-) Eintrag . . . :
151.189.21.100
www.arcor.de.
Eintragsname. . . . . : www.arcor.de
Eintragstyp . . . . . : 5
Gültigkeitsdauer. . . : 601
Datenlänge. . . . . : 4
Abschnitt . . . . . : Answer
CNAME-Eintrag . . . . :
www.arcor-online.net
Eintragsname. . . . . : www.arcor-online.net
Eintragstyp . . . . . : 1
Gültigkeitsdauer. . . : 601
Datenlänge. . . . . : 4
Abschnitt . . . . . : Answer
(Host-) Eintrag . . . :
151.189.21.100

Bild: Der Befehl ipconfig /displaydns

3.2. Netstat

Wenn ein von Ihnen betreuter Computer Netzwerkprobleme hat, sollte zunächst das Tool *netstat* liefert Protokollstatistiken und listet die aktuellen TCP/IP-Verbindungen.

netstat -a zeigt alle Verbindungen und die dazugehörigen Ports an.

*netstat -r zeigt d*en Inhalt der Routing-Tabelle mit Protokollstatistiken

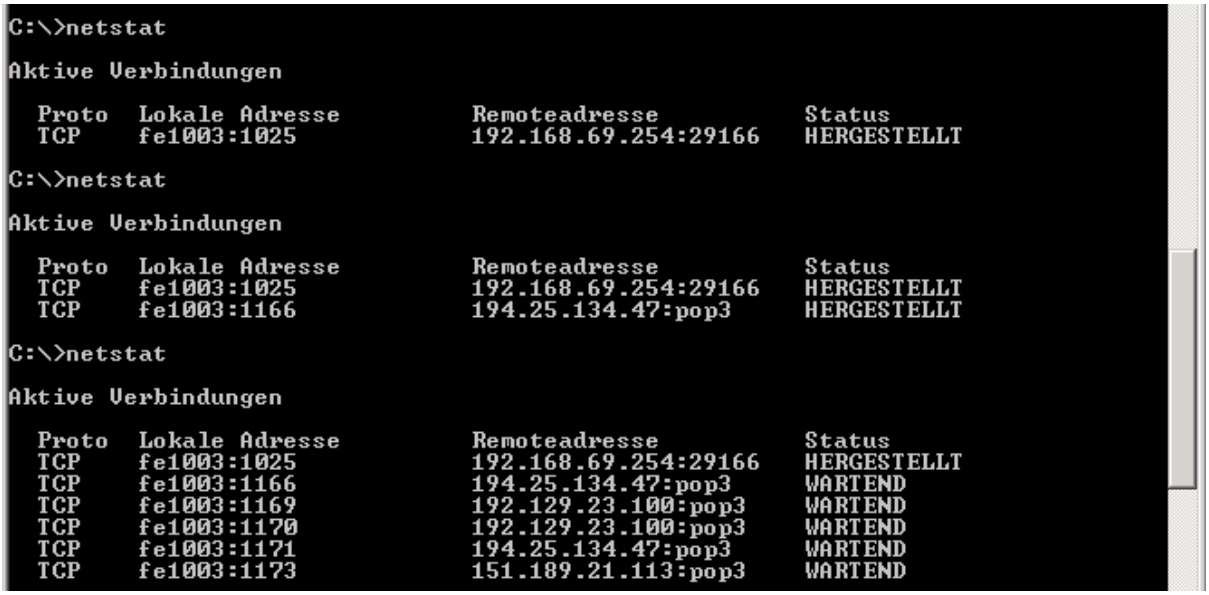


Bild: Der Befehl netstat

3.3. ping - Erreichbarkeitskontrolle für IP-Knoten

Ein ebenso einfaches wie wirkungsvolles Tool ist der Befehl ping. Mit ihm können Sie schnell feststellen, ob die TCP/IP-Verbindungen in Ihrem Netz funktionieren. Ein Ping auf die Loopback-Adresse 127.0.0.1 überprüft, ob TCP/IP auf dem lokalen Rechner korrekt installiert ist.

ping nutzt das Internet Control Message Protocol (ICMP), das nach RFC 792 spezifiziert ist. ICMP liefert Meldungen bezüglich Fehler bei der Übermittlung von IP-Frames und erlaubt damit eine Datenflusskontrolle.

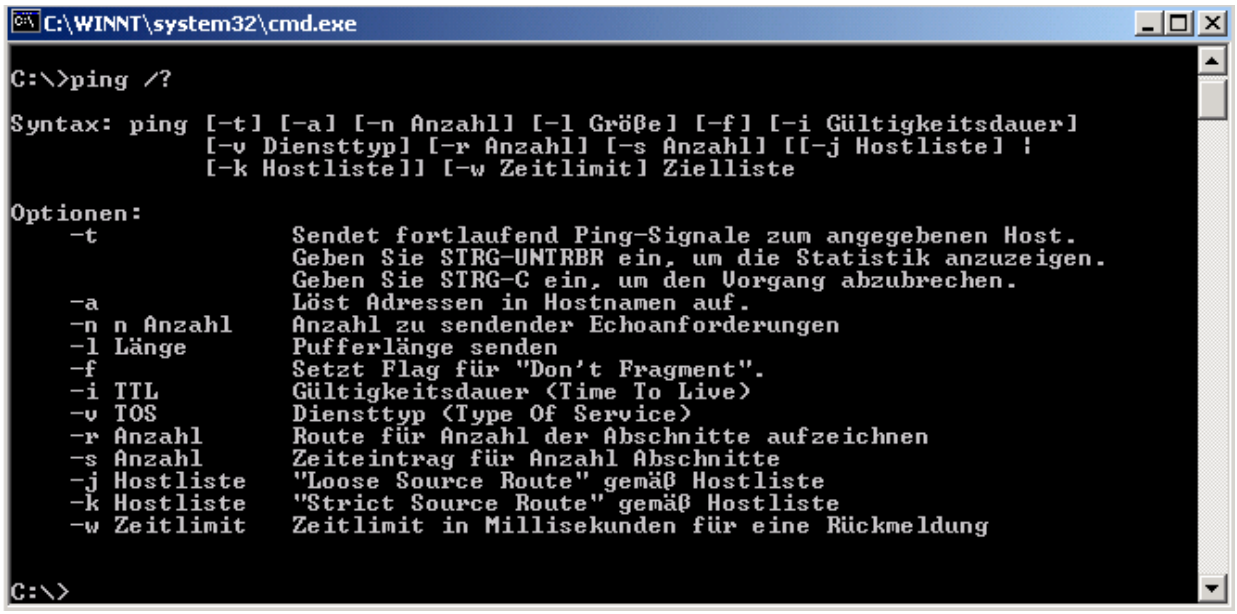

C:\WINNT\system32\cmd.exe
C:\>ping /?
Syntax: ping [-t] [-a] [-n Anzahl] [-l Größe] [-f] [-i Gültigkeitsdauer]
[-v Diensttyp] [-r Anzahl] [-s Anzahl] [[-j Hostliste] |
[-k Hostliste]] [-w Zeitlimit] Zielliste
Optionen:
-t Sendet fortlaufend Ping-Signale zum angegebenen Host.
Geben Sie STRG-UNTRBR ein, um die Statistik anzuzeigen.
Geben Sie STRG-C ein, um den Vorgang abzubrechen.
-a Löst Adressen in Hostnamen auf.
-n n Anzahl Anzahl zu sendender Echoanforderungen
-l Länge Pufferlänge senden
-f Setzt Flag für "Don't Fragment".
-i TTL Gültigkeitsdauer (Time To Live)
-v TOS Diensttyp (Type Of Service)
-r Anzahl Route für Anzahl der Abschnitte aufzeichnen
-s Anzahl Zeiteintrag für Anzahl Abschnitte
-j Hostliste "Loose Source Route" gemäß Hostliste
-k Hostliste "Strict Source Route" gemäß Hostliste
-w Zeitlimit Zeitlimit in Millisekunden für eine Rückmeldung
C:\>

Bild: Hilfeseite zum Befehl Ping

Wenn Sie den Computer mit seiner eigenen IP-Adresse anpingen, sehen Sie, ob die Netzwerkkarte vorschriftsmäßig arbeitet. Antworten das Gateway und die

anderen Subnetzstationen ebenfalls ohne größere Verzögerung, sollte auf dieser Ebene alles in Ordnung sein.

Fehlerszenario 1:

Mit dem Ping-Befehl können Sie zudem schnell herausfinden, ob es Probleme mit der Namensauflösung gibt: Funktioniert der Ping auf die IP-Adresse eines Rechners, der Ping auf seinen Host-Namen aber nicht, ist sehr wahrscheinlich die Namensauflösung fehlerhaft. In diesem Fall sollte die Konfiguration des Rechnernamens und seiner IP-Adresse im Domain Name Server überprüft werden.

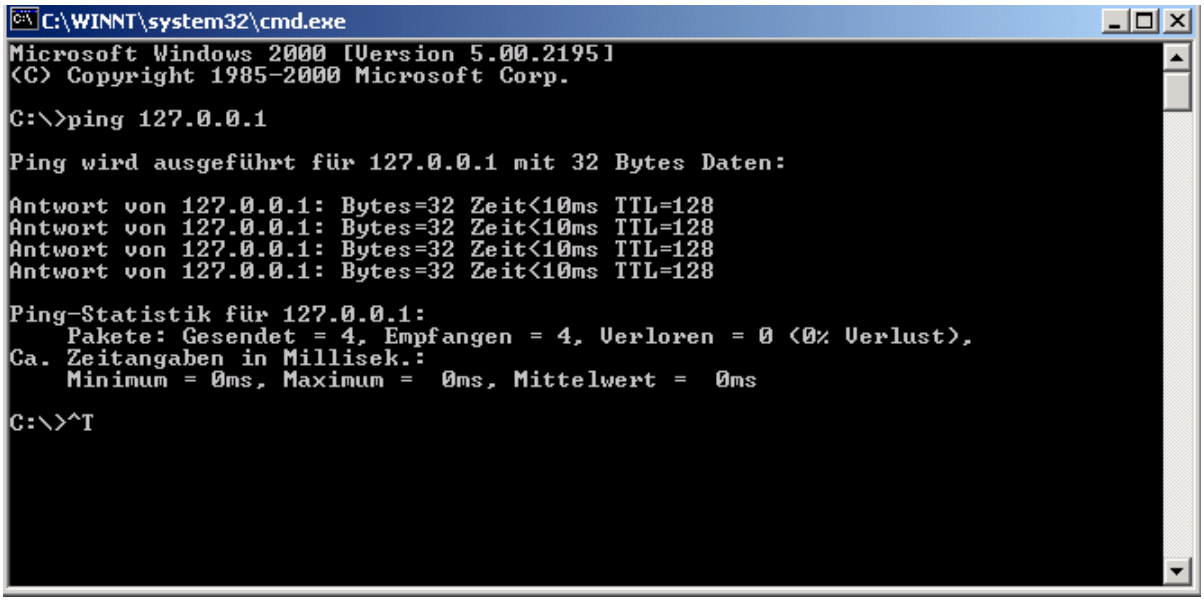


Bild: Ping auf die Loopback-Adresse

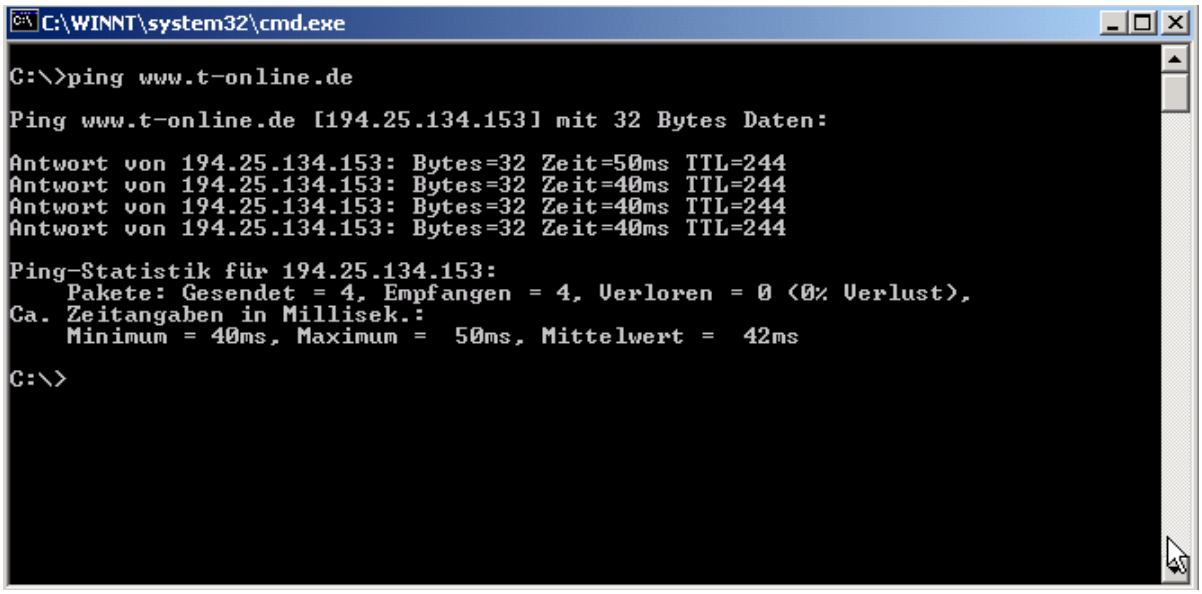


Bild: Ping auf eine Internet IP-Adresse

Fehlerszenario 2:

Zeigen die von Ihnen durchgeführten Pings Paketverluste im LAN oder liegen die Antwortzeiten dauerhaft im zweistelligen Millisekundenbereich, dürfte ein

Hardware-Fehler an einem Kabel, einer Netzwerkkarte oder einem Switch vorliegen.

Fehlerszenario 3: Rechner selbst nicht erreichbar

Ursache: Falsche Interface-Konfiguration, Lösung des Problems mit Hilfe von netstat, ifconfig bzw. ipconfig oder wincfg

Fehlerszenario 4: Lokale benachbarte Rechner nicht erreichbar

Ursache: Falsche IP-Konfiguration. Lösung durch Kontrolle der eingestellten IP-Adresse und der Subnetzmaske

Fehlerszenario 5: Router nicht erreichbar

Router-Problem

Fehlerszenario 6: Rechner hinter Router nicht erreichbar

Ursache: Falscher Eintrag des default-Gateways oder Router-Problem

3.4. route

Der Befehl route print zeigt die IP-Routing-Tabelle des jeweiligen Hosts an. Sie können die Routing-Tabelle mit Hilfe von route add und route delete verändern.

Die Option -p speichert neue Routen dauerhaft, -f löscht alle Gateway-Einträge aus der Tabelle. Vorhandene Routen werden mit change verändert.

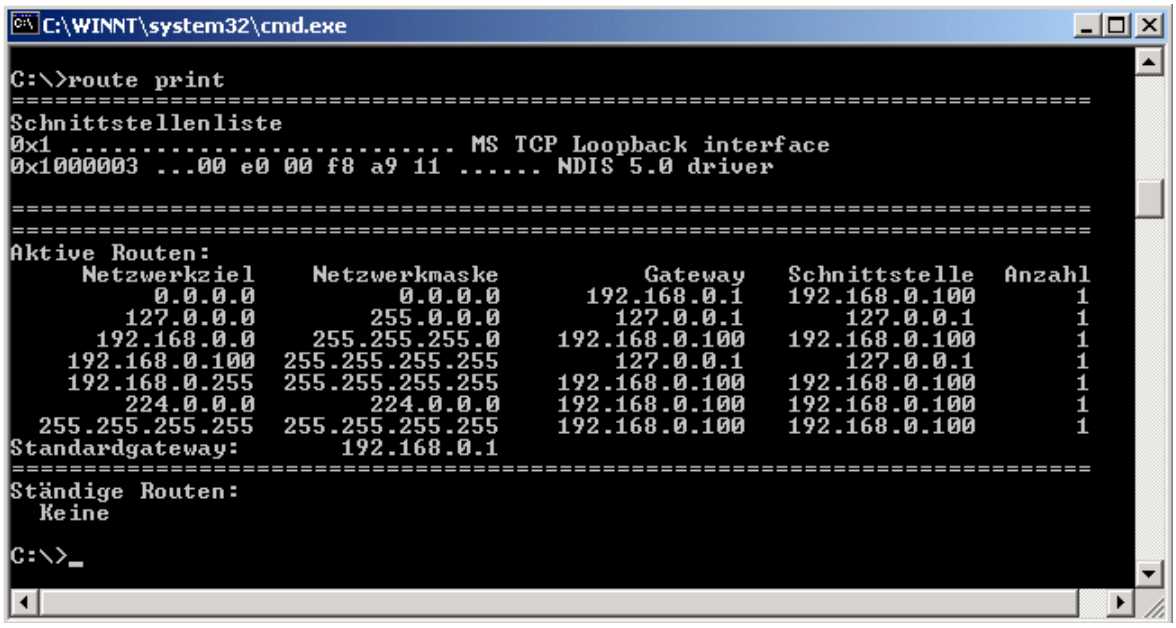


Bild: Ausgabe zum Befehl route print

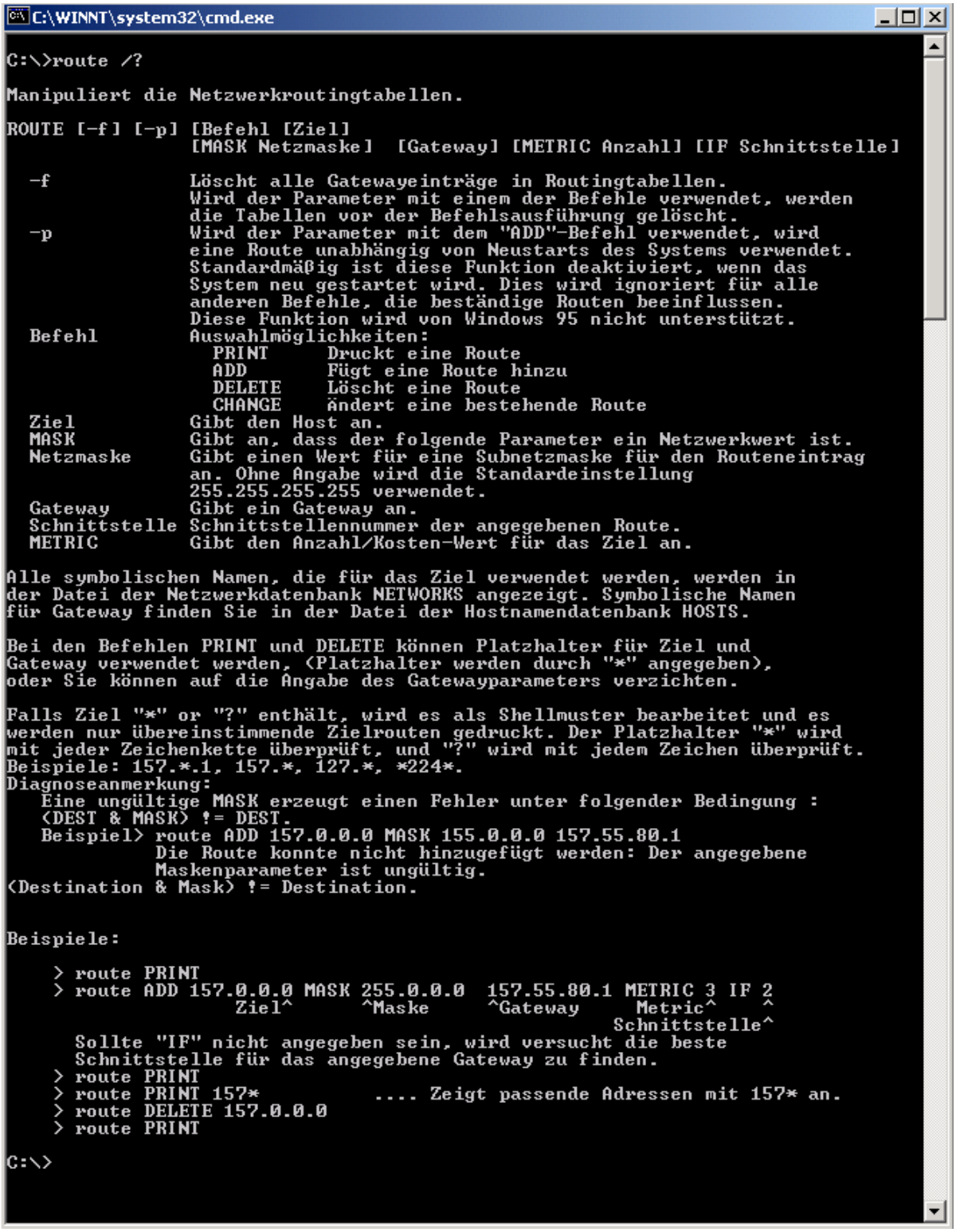

C:\WINNT\system32\cmd.exe
C:\>route /?
Manipuliert die Netzwerkroutingtabellen.
ROUTE [-f] [-p] [Befehl [Ziel]
[MASK Netzmaske] [Gateway] [METRIC Anzahl] [IF Schnittstelle]
-f Löscht alle Gatewayeinträge in Routingtabellen.
Wird der Parameter mit einem der Befehle verwendet, werden
die Tabellen vor der Befehlsausführung gelöscht.
-p Wird der Parameter mit dem "ADD"-Befehl verwendet, wird
eine Route unabhängig von Neustarts des Systems verwendet.
Standardmäßig ist diese Funktion deaktiviert, wenn das
System neu gestartet wird. Dies wird ignoriert für alle
anderen Befehle, die beständige Routen beeinflussen.
Diese Funktion wird von Windows 95 nicht unterstützt.
Befehl Auswahlmöglichkeiten:
PRINT Druckt eine Route
ADD Fügt eine Route hinzu
DELETE Löscht eine Route
CHANGE Ändert eine bestehende Route
Ziel Gibt den Host an.
MASK Gibt an, dass der folgende Parameter ein Netzwerkwert ist.
Netzmaske Gibt einen Wert für eine Subnetzmaske für den Routeneintrag
an. Ohne Angabe wird die Standardeinstellung
255.255.255.255 verwendet.
Gateway Gibt ein Gateway an.
Schnittstelle Schnittstellennummer der angegebenen Route.
METRIC Gibt den Anzahl/Kosten-Wert für das Ziel an.
Alle symbolischen Namen, die für das Ziel verwendet werden, werden in
der Datei der Netzwerkdatenbank NETWORKS angezeigt. Symbolische Namen
für Gateway finden Sie in der Datei der Hostnamendatenbank HOSTS.
Bei den Befehlen PRINT und DELETE können Platzhalter für Ziel und
Gateway verwendet werden, (Platzhalter werden durch "*" angegeben),
oder Sie können auf die Angabe des Gatewayparameters verzichten.
Falls Ziel "*" or "?" enthält, wird es als Shellmuster bearbeitet und es
werden nur übereinstimmende Zielrouten gedruckt. Der Platzhalter "*" wird
mit jeder Zeichenkette überprüft, und "?" wird mit jedem Zeichen überprüft.
Beispiele: 157.*.1, 157.*, 127.*, *224*.
Diagnoseanmerkung:
Eine ungültige MASK erzeugt einen Fehler unter folgender Bedingung :
(DEST & MASK) != DEST.
Beispiel> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1
Die Route konnte nicht hinzugefügt werden: Der angegebene
Maskenparameter ist ungültig.
(Destination & Mask) != Destination.
Beispiele:
> route PRINT
> route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
Ziel^ ^Maske ^Gateway Metric^ ^
Schnittstelle^
Sollte "IF" nicht angegeben sein, wird versucht die beste
Schnittstelle für das angegebene Gateway zu finden.
> route PRINT
> route PRINT 157* .... Zeigt passende Adressen mit 157* an.
> route DELETE 157.0.0.0
> route PRINT
C:\>

Bild: Hilfeseite zum Befehl route

3.5. tracert

Mit tracert erhalten Sie eine Liste aller Router, die auf dem Weg zwischen Ihrem Computer und der angegebenen Zieladresse liegen. Dabei werden allerdings nur die Router gelistet, die Pakete mit abgelaufenen TTL-Werten nicht verwerfen.

Zudem funktioniert tracert nur, wenn auf den beteiligten Routern und Firewalls die ICMP-Filter deaktiviert sind.

Der Befehl tracert zeigt somit den Weg eines Datenpakets von System A nach System B durch verfolgen der von ihm ausgesendeten UDP Pakete auf und gibt jede Zwischenstation (Router) aus.

tracert zeigt bei Fehlern die zuletzt erreichte Station (max. 30 Hops)

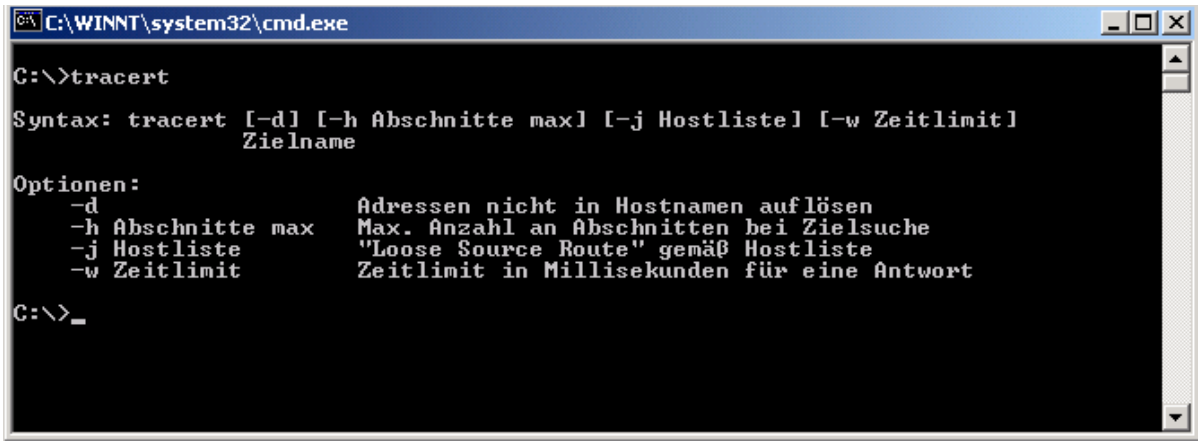

C:\WINNT\system32\cmd.exe
C:\>tracert
Syntax: tracert [-d] [-h Abschnitte max] [-j Hostliste] [-w Zeitlimit]
Zielname
Optionen:
-d Adressen nicht in Hostnamen auflösen
-h Abschnitte max Max. Anzahl an Abschnitten bei Zielsuche
-j Hostliste "Loose Source Route" gemäß Hostliste
-w Zeitlimit Zeitlimit in Millisekunden für eine Antwort
C:\>

Bild: Hilfesseite zum Befehl tracert

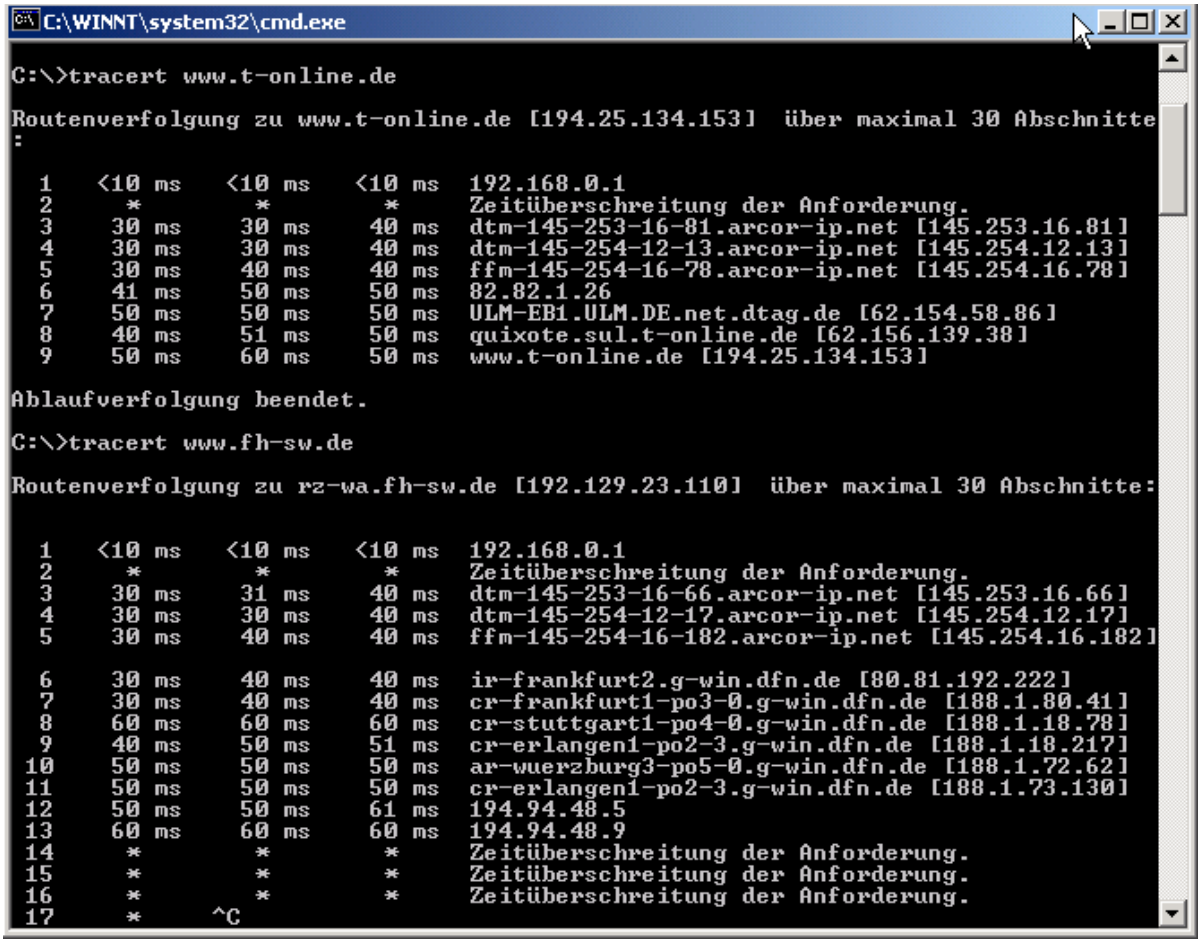

C:\WINNT\system32\cmd.exe
C:\>tracert www.t-online.de
Routenverfolgung zu www.t-online.de [194.25.134.153] über maximal 30 Abschnitte
:
1 <10 ms <10 ms <10 ms 192.168.0.1
2 * * * Zeitüberschreitung der Anforderung.
3 30 ms 30 ms 40 ms dtm-145-253-16-81.arcor-ip.net [145.253.16.81]
4 30 ms 30 ms 40 ms dtm-145-254-12-13.arcor-ip.net [145.254.12.13]
5 30 ms 40 ms 40 ms ffm-145-254-16-78.arcor-ip.net [145.254.16.78]
6 41 ms 50 ms 50 ms 82.82.1.26
7 50 ms 50 ms 50 ms ULM-EB1.ULM.DE.net.dtag.de [62.154.58.86]
8 40 ms 51 ms 50 ms quixote.sul.t-online.de [62.156.139.38]
9 50 ms 60 ms 50 ms www.t-online.de [194.25.134.153]
Ablaufverfolgung beendet.
C:\>tracert www.fh-sw.de
Routenverfolgung zu rz-wa.fh-sw.de [192.129.23.110] über maximal 30 Abschnitte:
1 <10 ms <10 ms <10 ms 192.168.0.1
2 * * * Zeitüberschreitung der Anforderung.
3 30 ms 31 ms 40 ms dtm-145-253-16-66.arcor-ip.net [145.253.16.66]
4 30 ms 30 ms 40 ms dtm-145-254-12-17.arcor-ip.net [145.254.12.17]
5 30 ms 40 ms 40 ms ffm-145-254-16-182.arcor-ip.net [145.254.16.182]
6 30 ms 40 ms 40 ms ir-frankfurt2.g-win.dfn.de [80.81.192.222]
7 30 ms 40 ms 40 ms cr-frankfurt1-po3-0.g-win.dfn.de [188.1.80.41]
8 60 ms 60 ms 60 ms cr-stuttgart1-po4-0.g-win.dfn.de [188.1.18.78]
9 40 ms 50 ms 51 ms cr-erlangen1-po2-3.g-win.dfn.de [188.1.18.217]
10 50 ms 50 ms 50 ms ar-wuerzburg3-po5-0.g-win.dfn.de [188.1.72.62]
11 50 ms 50 ms 50 ms cr-erlangen1-po2-3.g-win.dfn.de [188.1.73.130]
12 50 ms 50 ms 61 ms 194.94.48.5
13 60 ms 60 ms 60 ms 194.94.48.9
14 * * * Zeitüberschreitung der Anforderung.
15 * * * Zeitüberschreitung der Anforderung.
16 * * * Zeitüberschreitung der Anforderung.
17 * ^C

Bild: Der Befehl tracert

Fehlerszenario 1: Meldung „network unreachable“ und „no answer“

Lösung: Mit TRACERT den Verbindungsweg aufzeichnen und ggf. exteren Routing-Probleme detektieren

3.6. Der Befehl pathping

Das interessante Route-Tracing-Tool pathping kombiniert quasi die Funktionen von ping und tracert miteinander und liefert darüber hinaus zusätzliche Informationen.

Eingabeaufforderung
G:\Dokumente und Einstellungen\Administrator>pathping www.t-online.de
Routenverfolgung zu www.t-online.de [212.185.47.88]
über maximal 30 Abschnitte:
0 500mxp51 [192.168.111.51]
1 192.168.111.1
2 * * *
Berechnung der Statistiken dauert ca. 50 Sekunden...
Quelle zum Abs. Knoten/Verbindung
Abs. Zeit Verl./Ges.= % Verl./Ges.= % Adresse
0 500mxp51 [192.168.111.51]
0/ 100 = 0% |
1 2ms 0/ 100 = 0% 0/ 100 = 0% 192.168.111.1
100/ 100 =100% |
2 --- 100/ 100 =100% 0/ 100 = 0% 500mxp51 [0.0.0.0]
Ablaufverfolgung beendet.
G:\Dokumente und Einstellungen\Administrator>

Bild: pathping - Screenshot

Das Tool schickt über einen definierten Zeitraum hinweg Testpakete zu jedem Router, der auf dem Weg zu der angegebenen Endstation liegt. Diese Pakete werden vom jeweiligen Router wieder zurückgeschickt, wodurch pathping genau feststellen kann, an welcher Stelle im Übertragungspfad Pakete verloren gegangen sind. Damit ist es zum Beispiel möglich, einen überlasteten Router zu erkennen.

Kombiniert ping und tracert: Das Tool pathping ermittelt nicht nur die Route zur gewünschten Zielstation, sondern teilt auch genau mit, an welchen Stellen Pakete verloren gehen.

3.7. nslookup - Überprüfung der Namensauflösung

Für das Troubleshooting von DNS-Problemen, zum Beispiel bei der Namensauflösung von Hosts, ist das nslookup geeignet. Um die DNS-Konfiguration zu prüfen stehen zahlreiche Befehlsoptionen zur Verfügung. Ebenso kann ein Debug-Modus durch set debug oder durch set d2 aktiviert werden, im letzten Fall werden noch detailliertere Analysen ausgegeben.

Das Diagnosehilfsprogramm nslookup zeigt Informationen von DNS-Servern (DNS = Domain Name System), die auch als sog. Name-Server bezeichnet werden. DNS-

Servern stellen eine verteilte Datenbank von Host Informationen dar. Der Befehl nslookup ist nur verfügbar, wenn das Protokoll TCP/IP installiert wurde.

DNS- Konfiguration: Sie müssen z.B. dem lokalen Windows-Rechner mitteilen, wohin es seine DNS-Anfragen richten soll. Wenn Sie einen internen DNS-Server verwenden, sollten alle Clients auf diesen verweisen, andernfalls sollten Sie Ihre Firewall als DNS eintragen.

Es gibt zwei Arten, das Programm zu starten:

nslookup [domainname] oder nur nslookup

Mit der ersten Möglichkeit liefert nslookup den Name-Server-Eintrag zu genau einem Rechner, der dem Programm als Parameter übergeben wird. Im zweiten Fall landet man im interaktiven Modus und kann dem Programm Befehle erteilen und so auch mehrere Einträge abrufen. Beenden des interaktiven Modus durch Eingabe von exit oder <CTRL-D>.

Nslookup unterstützt u. a. folgende Funktionen:

- Wenn man ihm einen URL-Namen angibt, liefert es die IP-Adresse zurück.
- Bei Angabe der IP-Adresse liefert es den DNS-Namen.
- Auf den Domänen-Namen liefert es die zugehörigen DNS-Server für diese Domäne.

Szenario 1:

nslookup www.fh-sw.de

Antwort: Address: 192.129.23.110

Wenn zu einer bekannten IP-Adressen der zugehörige Domain-Name aufgefunden werden soll, muss nslookup mit dem Befehl set query=ptr in den entsprechenden Modus umgeschaltet werden. Die IP-Adresse wird anschließend in umgekehrter Reihenfolge und mit dem Zusatz in-addr.arpa eingegeben.

Szenario 2:

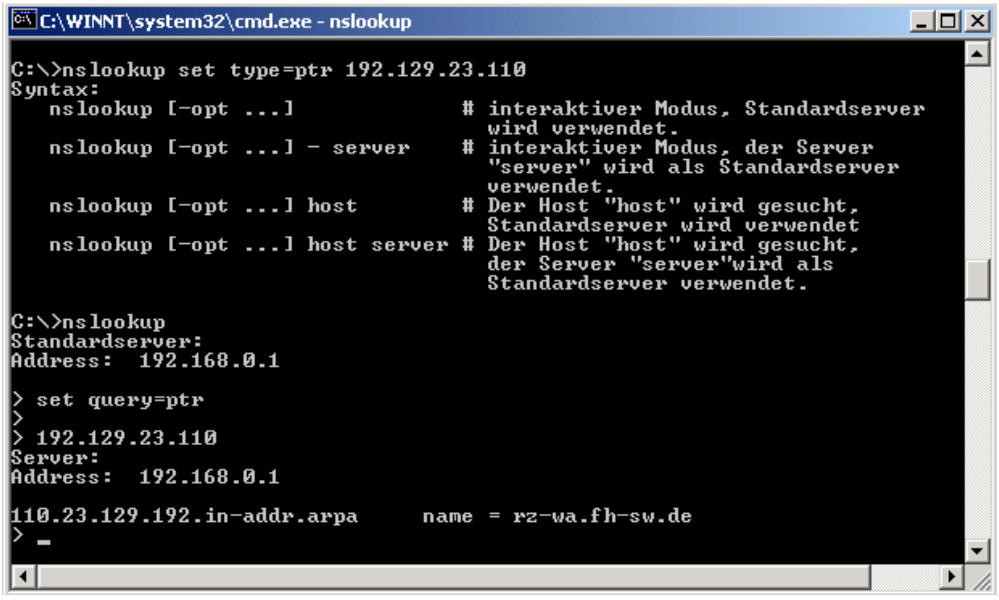
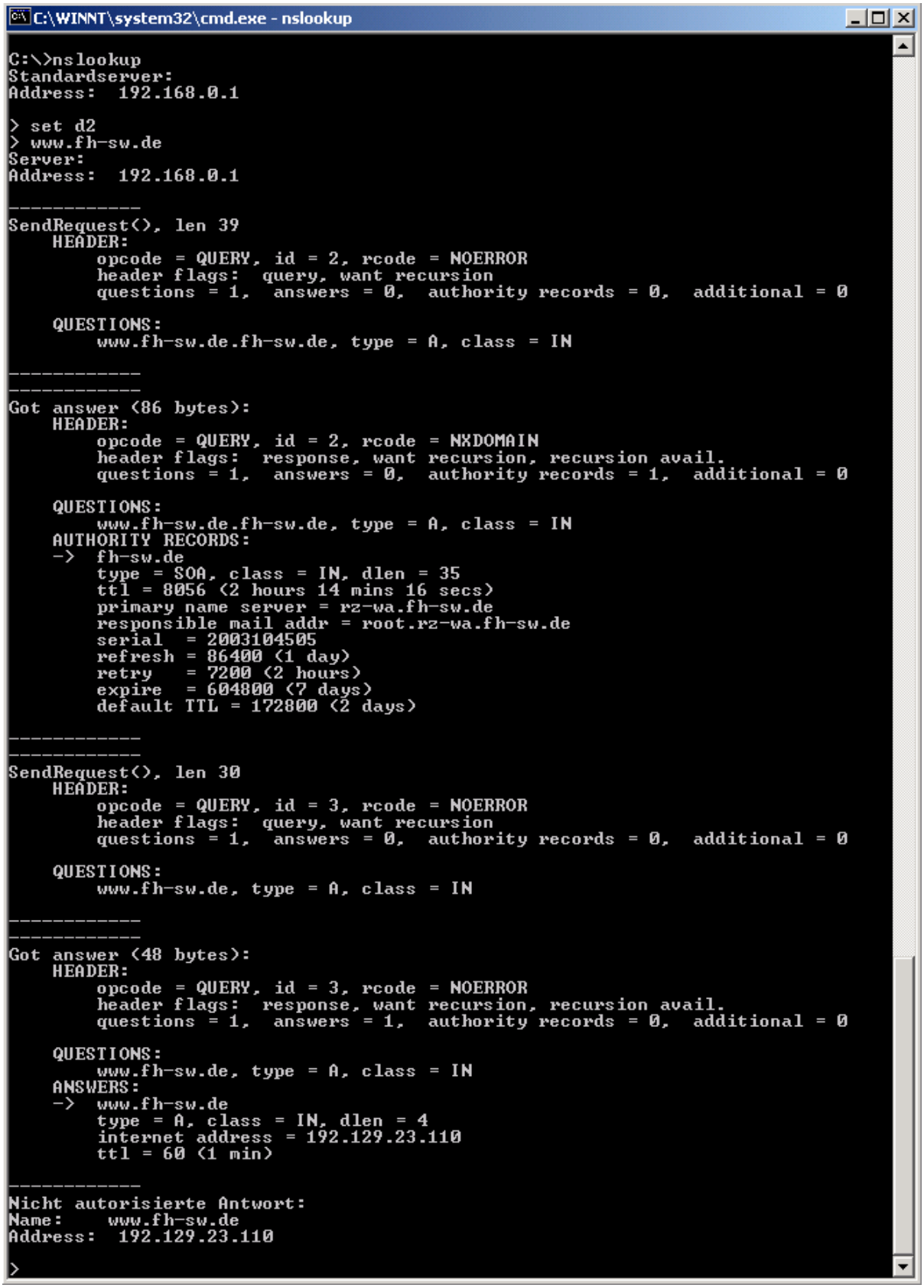

C:\WINNT\system32\cmd.exe - nslookup
C:\>nslookup set type=ptr 192.129.23.110
Syntax:
nslookup [-opt ...] # interaktiver Modus, Standardserver wird verwendet.
nslookup [-opt ...] - server # interaktiver Modus, der Server "server" wird als Standardserver verwendet.
nslookup [-opt ...] host # Der Host "host" wird gesucht, Standardserver wird verwendet
nslookup [-opt ...] host server # Der Host "host" wird gesucht, der Server "server"wird als Standardserver verwendet.
C:\>nslookup
Standardserver:
Address: 192.168.0.1
> set query=ptr
>
> 192.129.23.110
Server:
Address: 192.168.0.1
110.23.129.192.in-addr.arpa name = rz-wa.fh-sw.de
>

Bild: Screenshot nslookup

C:\WINNT\system32\cmd.exe - nslookup
> nslookup /?
Unrecognized command: nslookup /?
> nslookup
C:\>nslookup
Standardserver:
Address: 192.168.0.1
> ?
Befehle: (Kennungen werden in Großbuchstaben angezeigt, [] steht für optional)
NAME - Info über Host/Domäne NAME
(verwendet Standardserver)
NAME1 NAME2 - Wie oben; verwendet NAME2 als Server
help oder ? - Info über allgemeine Befehle; siehe auch
nslookup(1)
set OPTION - Legt eine Option fest
all - Zeigt alle Optionen, aktuelle Server und
Hosts an
[no]debug - Zeigt Debuginformationen an
[no]d2 - Zeigt ausführliche Debuginformationen an
[no]defname - Fügt jeder Abfrage den Domänenname an
[no]recurse - Rekursive Antwort auf Anfrage
[no]search - Verwendet die Domänensuchliste
[no]vc - Verwendet immer einen "virtual circuit"
domain=NAME - Legt den Standarddomänennamen mit NAME fest
srchlist=N1[/N2/.../N6] - Legt Domäne mit N1 und Suchliste mit
N1,N2.. fest
root=NAME - Legt den Stammserver mit NAME fest
retry=X - Legt die Anzahl der Neuversuche mit X fest
timeout=X - Legt das erste Zeitüberschreitungsintervall
mit X Sekunden fest
querytype=X - Legt den Abfragetyp fest, z.B.
A,ANY,CNAME,HINFO,NS,SOA,WKS
type=X - Synonym mit "querytype"
class=X - Legt die Abfrageklasse mit IN, CHAOS,
HESIOD oder ANY fest
server NAME - Legt mit dem akt. Server den Standardserver
mit NAME fest
lserver NAME - Legt mit dem 1. Server den Standardserver
mit NAME fest
finger [USER] - Führt den Befehl "finger" für NAME aus
root - Legt den aktuellen Standardserver mit
"root" fest
ls [opt] DOMÄNE [> DATEI] - Zeigt Adressen in DOMÄNE an
(Ausgabe in DATEI)
-a - Führt kanonische Namen und Aliase auf
-d - Führt alle Einträge auf
-t TYP - Führt die Einträge des Typs auf
(z.B. A, CNAME, MX, usw.)
view DATEI - Sortiert eine "ls"-Outputdatei und zeigt
sie mit "pg" an
exit - Beendet das Programm, auch EOF (z.B. ^D)
möglich
> _

Bild: Hilfeseite zum Befehl nslookup


C:\WINNT\system32\cmd.exe - nslookup
C:\>nslookup
Standardserver:
Address: 192.168.0.1
> set d2
> www.fh-sw.de
Server:
Address: 192.168.0.1

SendRequest(), len 39
HEADER:
opcode = QUERY, id = 2, rcode = NOERROR
header flags: query, want recursion
questions = 1, answers = 0, authority records = 0, additional = 0
QUESTIONS:
www.fh-sw.de.fh-sw.de, type = A, class = IN

Got answer (86 bytes):
HEADER:
opcode = QUERY, id = 2, rcode = NXDOMAIN
header flags: response, want recursion, recursion avail.
questions = 1, answers = 0, authority records = 1, additional = 0
QUESTIONS:
www.fh-sw.de.fh-sw.de, type = A, class = IN
AUTHORITY RECORDS:
-> fh-sw.de
type = SOA, class = IN, dlen = 35
ttl = 8056 (2 hours 14 mins 16 secs)
primary name server = rz-wa.fh-sw.de
responsible mail addr = root.rz-wa.fh-sw.de
serial = 2003104505
refresh = 86400 (1 day)
retry = 7200 (2 hours)
expire = 604800 (7 days)
default TTL = 172800 (2 days)

SendRequest(), len 30
HEADER:
opcode = QUERY, id = 3, rcode = NOERROR
header flags: query, want recursion
questions = 1, answers = 0, authority records = 0, additional = 0
QUESTIONS:
www.fh-sw.de, type = A, class = IN

Got answer (48 bytes):
HEADER:
opcode = QUERY, id = 3, rcode = NOERROR
header flags: response, want recursion, recursion avail.
questions = 1, answers = 1, authority records = 0, additional = 0
QUESTIONS:
www.fh-sw.de, type = A, class = IN
ANSWERS:
-> www.fh-sw.de
type = A, class = IN, dlen = 4
internet address = 192.129.23.110
ttl = 60 (1 min)

Nicht autorisierte Antwort:
Name: www.fh-sw.de
Address: 192.129.23.110
>

Bild: Erweiterte Debuginformationen durch “set d2“

3.8. nbtstat - NetBIOS Namentests

Das Werkzeug nbtstat eignet sich für das Troubleshooting bei Problemen mit der Auflösung von NetBIOS-Namen in IP-Adressen. Mit diesem Tool können fehlerhafte Einträge entfernt oder korrigiert werden.

Nbtstat –c zeigt das im Namens-Cache gespeicherte Mapping von NetBIOS-Namen zu IP-Adressen an.

Nbtstat –R entleert den Namens-Chache und lädt alle #PRE-Einträge aus der LMHOSTS-Datei neu.

4. NETZWERK-FEHLERSZENARIEN

4.1. Fehlerbild: Unerreichbarkeit von IP-Stationen

Fehlerbild:

Eingabe am Rechner A: Ping 149.224.11.1

- Fehlermeldung: Host Unreachable, ARP failed

Eingabe am Rechner A: Ping 149.225.11.1

- Host responding

Fehlerbild: Kommunikation über zwei Router erfolgreich, nicht jedoch über einen Router!

Eingabe am Rechner B: Ping 149.224.11.1

- Host responding

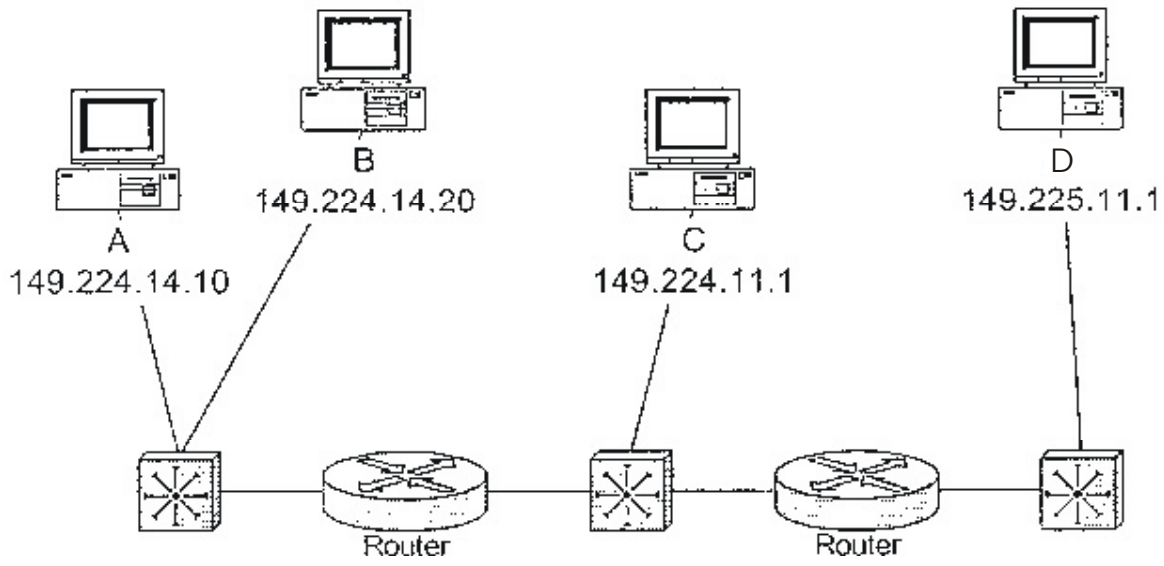


Bild: Szenario: Unerreichbarkeit von IP-Stationen

Messung mit Protokollanalysator:

Eingabe am Rechner A:

- Ping 149.224.11.1 : ARP-Request wird erfolgreich durchgeführt
- Ping 149.225.11.1 : Packet wird an die MAC-Adresse des Routers gesendet

Kontrolle der Konfiguration von Rechner A ergibt: Subnetzmaske 255.255.0.0

- 149.224.11.1 wird als Adresse im *eigenen* Subnetz erkannt
- 149.225.11.1 wird als Adresse im *fremden* Subnetz erkannt

Abhilfe:

Subnetzmaske von Rechner A umstellen auf 255.255.255.0

- Auch Rechner C wird damit als Rechner in fremdem Subnetz eingestuft, A sendet Pakete an den ersten Router

4.2. Fehlerbild: Unerreichbarkeit von IP-Stationen

Fehlerbild:

Anwender B klagt über Performance-Nachteile gegenüber Anwender C beim Zugriff auf Server D.

Hardwareaustattung der Anwender B und C ist identisch

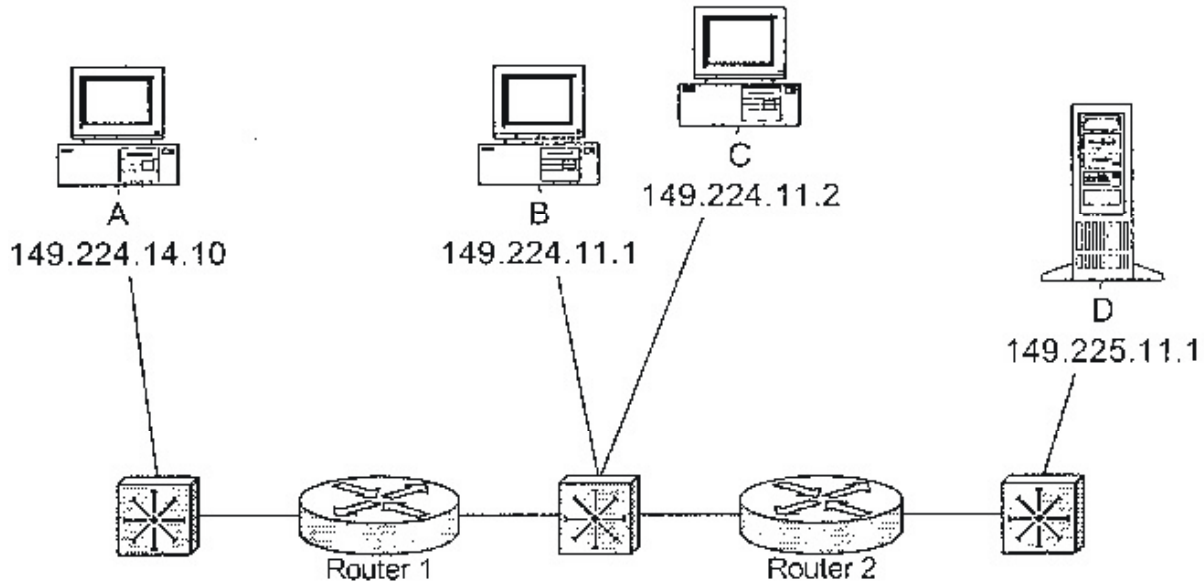


Bild: Szenario: Unerreichbarkeit von IP-Stationen

Messung mit dem Protokollanalysator:

Messung ergibt:

- Rechner B adressiert Router 1
- Rechner C adressiert Router 2
- Router 1 sendet ICMP-„Redirect“ an Rechner B
- Router 1 leitet Pakete von B an Router 2 weiter

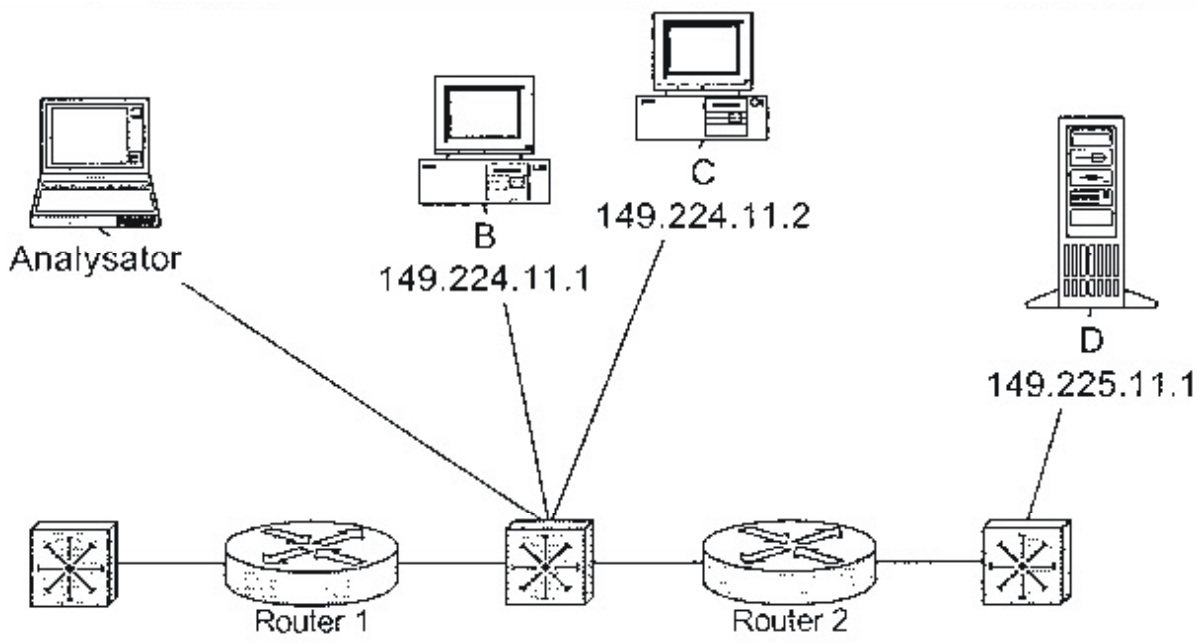


Bild: Messung mit dem Protokollanalysator

Ursache:

Einige TCP/IP-Stacks können ICMP-„Redirect“ nicht korrekt verarbeiten.

Übertragung der gleichen Datenmenge benötigt bei Anwender B mindestens die doppelte Zeit, bei 2 Hops die dreifache Zeit u.s.w.. Das Problem wird durch Protokolle vermindert, die nicht auf jedes Paket eine Quittung verlangen (z.B. UDP)

Wichtig deshalb: Hop-Counts im Netzwerk sollten durch ein Netzwerkmanagement-tool überwacht werden.

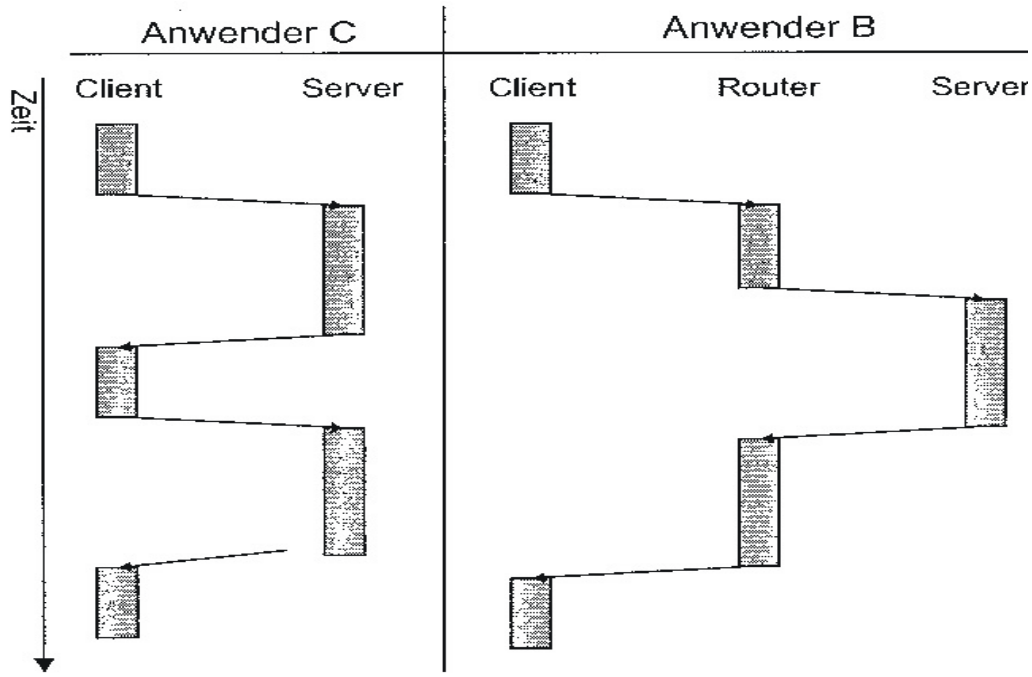


Bild: Einfluss des Hop-Count auf die Performance

Abhilfe:

- Einträge der Default-Router (default-Gateway) kontrolliert vornehmen,. d. h.
  Zentrale Einstellung per DHCP
  Evtl. mehrere Default-Router („Dead Gateway Detection“) konfigurieren.
- ICMP-Redirects permant mit Netzwerkmanagementtools überwachen, damit Performance sichergestellt wird.

5. ZUSAMMENFASSUNG

5.1. Häufige Fehlerursachen bei Koaxialverkabelung (Layer 1):

- fehlender/Defekter Abschlusswiderstand
- Kabel zu lang
- physikalische Beschädigung des Kabels
- fehlende/falsche Erdung
- Kabel ist unterbrochen
- Kabel geknickt
- elektromagnetische Störung

Häufige Fehlerursachen bei Twisted-Pair-Verkabelung (Layer 1):

- Kabel zu lang (hohe Dämpfung)
- defekte Patchkabel/Endgerätekabel (Knick, physikalische Beschädi
- gung)
- falsche PIN-Belegung am Stecker
- Kabel stellenweise nicht verdrillt
- elektromagnetische Störung
- defekte Netzwerkkarte
- defekter Port an der Netzwerkkomponente

Häufige Fehlerursachen bei LWL-Verkabelung

- Kabel zu lang (hohe Dämpfung)
- zu viele Patchungen (hohe Dämpfung)
- Fasern sind vertauscht
- Stecker verschmutzt (hohe Dämpfung)
- Adernbruch
- zu geringe Lichtleistung der Netzwerkkomponente
- defekter Port an der Netzwerkkomponente

5.2. Häufige Fehlerursachen bei Ethernet (Layer 2):

- Defekte Netzwerkkarten
- elektromagnetische Störungen
- Kabel defekt, geknickt, zu lang
- falsche Erdung
- falsche Konfiguration auf Netzwerkkomponenten (Geschwindigkeit,
- Duplex, Filtereinstellungen
- Überlastung von Netzwerkkomponenten
- schlechtes Netzdesign

5.3. Häufige Fehlerursachen bei IP (Layer 3):

- TCP/IP nicht korrekt installiert
- falsche IP-Adresse
- falsche Subnetzmaske
- falsches Default-Gateway
- Router-Port nicht aktiv
- fehlerhafte Accessliste/Filter auf Router

- unbekanntes Zielnetz
- doppelte IP-Adressen
- Netzüberlastung
- Überlastung von Routern
- Routerprozess nicht aktiv
- unterschiedliche Timer-Werte bei Routern